Strategy Research Project

Cyber Operations and the Warfighting Functions

by

Lieutenant Colonel Walter S. Sutton
United States Army

United States Army War College
Class of 2013

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
xx-03-2013

2. REPORT TYPE
STRATEGY RESEARCH PROJECT

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Cyber Operations and the Warfighting Functions

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Walter S. Sutton
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Charles J. Tulaney
United States Marine Corps

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,855

14. ABSTRACT

In 2005, the Department of Defense recognized cyberspace as the fifth operational domain. In 2009, the Commander of U.S. Strategic Command directed the creation of U.S. Cyber Command on the heels of recently reported cyber attacks against Estonia and Georgia. These cyber attacks negatively affected the state’s ability to provide effective governance. Sovereign nations across the world took notice. Cyber terrorism, at best cyber hacktivism, had crossed the threshold to embody what most consider acts of war. This strategic research paper utilizes the Estonia and Georgia cyber attacks to observe how cyber forces draw on the joint functions like a Brigade Combat Team or Air Expeditionary Wing uses the functions in their respective domains. The paper briefly describes cyber criminal activity, cyber hacktivism, and cyber terrorism to differentiate those activities from offensive cyber operations. The paper succinctly discusses U.S. Cyber Command’s three mission areas, further defining the discipline of military offensive cyber operations. The paper then explores how Joint Force Commanders may utilize the joint / warfighting functions depicted in Joint and Army doctrine to integrate and synchronize offensive cyber operations.

15. SUBJECT TERMS
Joint Functions, Cyber Rules of Engagement, Cyber ROE

16. SECURITY CLASSIFICATION OF:

a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**
UU	UU	UU

17. LIMITATION OF ABSTRACT
UU

18. NUMBER OF PAGES
32

19a. NAME OF RESPONSIBLE PERSON

19b. TELEPHONE NUMBER *(Include area code)*

USAWC STRATEGY RESEARCH PROJECT

Cyber Operations and the Warfighting Functions

by

Lieutenant Colonel Walter S. Sutton
United States Army

Colonel Charles J. Tulaney
United States Marine Corps
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Cyber Operations and the Warfighting Functions
Report Date:	March 2013
Page Count:	32
Word Count:	5,855
Key Terms:	Joint Functions, Cyber Rules of Engagement, Cyber ROE
Classification:	Unclassified

In 2005, the Department of Defense recognized cyberspace as the fifth operational domain. In 2009, the Commander of U.S. Strategic Command directed the creation of U.S. Cyber Command on the heels of recently reported cyber attacks against Estonia and Georgia. These cyber attacks negatively affected the state's ability to provide effective governance. Sovereign nations across the world took notice. Cyber terrorism, at best cyber hacktivism, had crossed the threshold to embody what most consider acts of war. This strategic research paper utilizes the Estonia and Georgia cyber attacks to observe how cyber forces draw on the joint functions like a Brigade Combat Team or Air Expeditionary Wing uses the functions in their respective domains. The paper briefly describes cyber criminal activity, cyber hacktivism, and cyber terrorism to differentiate those activities from offensive cyber operations. The paper succinctly discusses U.S. Cyber Command's three mission areas, further defining the discipline of military offensive cyber operations. The paper then explores how Joint Force Commanders may utilize the joint / warfighting functions depicted in Joint and Army doctrine to integrate and synchronize offensive cyber operations.

Cyber Operations and the Warfighting Functions

> …the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.
>
> —President Barack Obama
> Remarks by the President on Securing Our Nation's Cyber Infrastructure[1]

The cyber attacks on Estonia and Georgia negatively affected their ability to provide effective governance. Nations across the world took notice. Cyber terrorism, or at best cyber hacktivism, had crossed the threshold to embody what most sovereign nations consider acts of war. The Estonia and Georgia cyber attacks were not happenstance events, rather planned, integrated, and synchronized operations to achieve intended effects. The joint functions / warfighting functions provide an operational framework for Joint Force Commanders (JFC) to coordinate, integrate, and synchronize cyber operations. The ensuing analysis illustrates that cyber operations share many of the same qualities as the more traditional operations in the land, sea, air, and space domains. But, before any analysis can begin, we must review a few key actions the military has taken over the last ten years, define what constitutes cyberspace, and understand how cyber operations differs from cyber crimes, cyber hacktivism, and cyber terrorism.

In 2005, the Department of Defense (DoD) recognized cyberspace as the fifth operational domain, a move that brought cyber operations from a largely supporting effort into an operational space equal to the land, sea, air, and space domains.[2] Cyber operations certainly existed prior to 2005, but in the past decade, the United States

Government has become increasingly more reliant on cyberspace to manage its governance responsibilities. The Executive Branch's International Strategy for Cyber Space defines the importance of cyberspace stating, the "Digital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies."[3] However, America's cyberspace reliance creates strategic weaknesses our governmental leaders must address and mitigate. The cyber attacks on Estonia and Georgia only serve to highlight these strategic vulnerabilities.

In 2007, Estonia received a distributed denial of service attack so severe that their Foreign and Justice Ministry's websites were all but completely inaccessible. Estonia's cyber counter-mitigation efforts were unsuccessful; to restore internal national Internet service to their citizenry, the Estonian Government terminated their connections to the global Internet.[4] Similarly, in 2009, Georgia received a distributed denial of service attack crippling their governmental web sites rendering them inaccessible. The interesting point here is that this attack happened to coincide with the Russian Military moving into South Ossetia – a rebel region in Georgia.[5] Given these successive events and recognizing cyber as the fifth domain, the Secretary of Defense ordered the Commander of U.S. Strategic Command to establish a command to direct the operations and defense of specified DoD information networks and, when directed conduct full spectrum military operations in cyberspace.[6]

In 2009, the Commander of U.S. Strategic Command established U.S. Cyber Command to plan, synchronize, and direct activities to operate and defend the DoD networks "in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries."[7] To accomplish these tasks, U.S. Cyber Command (USCYBERCOM) established an operational framework consisting of three distinct discipline areas: DoD Information Network Operations, Defensive Cyberspace Operations, and Offensive Cyberspace Operations. The DoD Information Network Operations (DINO) discipline area embodies activities to design, build, configure, secure, operate, and maintain and sustain DoD networks to create and preserve information assurance on the DOD information networks. The Defensive Cyberspace Operations (DCO) discipline area consists of passive and active cyberspace operations intended to preserve the ability to utilize the friendly cyberspace capabilities and protect data, networks, and net-centric capabilities. The Offensive Cyberspace Operations (OCO) discipline area incorporates all operations conducted to project power against adversaries in or through cyberspace. These three discipline areas contain distinct military tasks and in certain cases military operations. These tasks will be discussed in detail later in the paper; however, in order to begin the discussion about cyber operations, we must first define what cyberspace is and what role DoD has in cyberspace.

Cyberspace and the Cyber Domain

A brief discussion on what constitutes cyberspace and how it is manifested in the operational environment is appropriate before a discussion can be begin with respect to cyber criminality, cyber hacktivism, cyber terrorism, and cyber operations. Joint Publication (JP) 1-02 defines cyberspace as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[8] JP 1-02's definition of cyberspace includes the information environment itself, the transport networks (including but far beyond the public Internet), and computers (all digital and electronic devices) inclusive of the embedded hardware and software. The Joint Publication Capstone Concept for Joint Operations (CCJO v2.0) first recognized Cyberspace as a separate domain in 2005.[9] DoD's acknowledgment of cyberspace as an operational domain is critical to the understanding that U.S. Military cyber forces are targeting and influencing our adversaries digital/electronic systems. The CCJO v2.0 solidifies this concept by identifying domains as "any potential operating "space" through which the target system can be influenced."[10] The CCJO v2.0 further stipulates that synonymous with the land, sea, air, and space domains, the United States must "maintain our dominance in the cyber domain."[11] The military's task of maintaining cyber dominance is extremely difficult at best, as our "future adversaries will seek the space between clearly combatant and clearly criminal to avoid our traditional military strengths."[12] I contend the space between clearly combatant and clearly criminal is not nearly as clean as that statement might portray. Therefore, it is important to understand the differences between cyber crime, cyber hacktivism, cyber terrorism, and, for military purposes, cyber operations.

Cyber Criminal Activity, Cyber Hacktivism, Cyber Terrorism, and Cyber Operations

Cyber crime, cyber hacktivism, cyber terrorism, and cyber operations boundaries are admittedly very blurred. In order to frame the discussion of the joint functions correctly, I will define the terms using documented definitions with a supporting albeit simple example to illustrate each concept. These definitions will assist in framing the warfighting function discussions discussed later.

Bonnie Adkins defined cyber crime as activities that range "from illegal exploration, hacking or other computer intrusions perpetrated by an individual or group with criminal or self-motivated interests and intent."[13] Personal identity theft and industrial/corporate espionage (for purposes other than harm to national security) best exemplify cyber crime. Although individuals and businesses may suffer financially devastating and extreme personal hardships as a result of cyber crime, these acts are usually not oriented to matters of national security. Unless America's national security (or economic security to the extent that it impacts our national security) is challenged or our adversaries attacks the .mil network, the DoD will defer responsive action to appropriate agency(ies) or organization(s). When it comes to application of military force, the DoD is governed by rules of engagement (ROE) "that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered."[14] Until recently, the focal point of the ROE was oriented toward the traditional forces that operate in the land, sea, air, and space domains. Recently USCYBERCOM has begun working with the DoD and the current political administration for establishing CYBER ROE and criteria upon which USCYBERCOM will act.[15] With an established CYBER ROE, USCYBERCOM will be better positioned to develop effective strategies for events that require DoD involvement, how and to what extent the DoD will commit cyber forces against an adversary, and what constitutes a measured response to a cyber attack.

Dorothy Denning, in her article *Activitism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, defines cyber hacktivism as "the marriage of hacking and activism. It covers operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage."[16] Perhaps the best example of combining cyber hacktivism and cyber activism is the environmental activist group Decocidio who hacked the European Climate Exchange's website in protest of the practice of carbon trading. Decocidio hacked the European Climate Exchange's website and replaced the Exchange's correct webpage with Decocidio's own webpage in order to bring awareness about carbon trading as a "dangerous false solution to the climate crisis."[17] Decocidio did not want personal or corporate advantage nor were they interested in encroaching on participating country's national security. Decocidio's actions were primarily one of social activism played out in a digital domain.

Ms. Denning defines cyber terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein…to intimidate or coerce a government or its people in furtherance of political or social objectives."[18] Ms. Denning goes on to say that, attacks "should result in violence against persons or property, or at least cause enough harm to generate fear."[19] Cyber terrorist attacks on supervisory control and data acquisition (SCADA) systems typify attacks that would cause enough harm to generate fear in the intended populace. Cyber terrorists recently (discovered on 8 November 2011) hacked into the Springfield, Illinois city water utilities SCADA system,[20] and while cyber terrorist hacking into a water SCADA system does not in-and-of-itself inspire a lot of fear in the population, Joe Weiss of Applied Control Systems commented that it is important to identify who made the SCADA system that was hacked. Mr. Weiss made the comment that "if this is a [big software vendor], this could be so ugly, because a [big software vendor] would have not only systems in water utilities but a [big software vendor] could even be [used] in nukes."[21] Cyber terrorists with access to nuclear power plant's SCADA systems would most certainly create a large amount of panic in the American populace. As you can see, cyber terrorism's objective is intimidation or coercion of a government or its people in furtherance of political or social objectives, not for personal or corporate gain. Although cyber terrorism could potentially produce mass public confusion which might be sufficient to justify employment of national assets for rectification, a cyber terrorist's intention is not necessarily to attack national security. Cyber terrorism is an act that rides the fine line between political/social activism and hostile political regime conflict. In the example above, one could construe cyber terrorism against a nuclear power SCADA system as an act against our national security. Our reactionary cyber forces, in this example, would benefit greatly from a defined cyber ROE affording them immediate response times in thwarting the SCADA attack event as well as knowing what constituted an appropriate measured response.

U.S. Military cyber operations are quite different from cyber crime, cyber hacktivism, and cyber terrorism. Cyber forces conduct operations, like their counterparts in land, sea, air, and space domains, by effectively applying combat power to achieve intended results. Cyber forces "generate combat power by converting potential into effective action."[22] Combat power, as defined in JP 3-0, is the "the total means of destructive and/or disruption force which a military unit/formation can apply against the opponent at a given time."[23] Cyber forces generate and apply combat power through destructive or disruptive actions against an adversary to "overcome and achieve periods of cyber space superiority or domination at a time and place of the commander's choosing in order to successfully continue execution of operations."[24] Cyber forces apply combat power either through defensive operations like defending key terrain –

equivalent to defensive measures for protecting a web server farm hosting command and control information, or through offensive operations where seizing key terrain maybe desired – equivalent to gaining access to the adversary’s command and control web servers and exfiltrating information. JP 1-02 defines key terrain as an area where the seizure or retention of “affords a marked advantage to either combatant.”[25] Using the example above, command and control servers and the associated information constitute key terrain in cyberspace. Having access to an adversary’s command and control hardware affords us a marked advantage over our adversary. USCYBERCOM created an operational framework around the concepts of the activities it takes to operate the military networks, defensive operations, and offensive operations.

USCYBERCOM’s Operational Framework

USCYBERCOM’s operational framework serves to synchronize and deconflict activities between the discipline areas. The DoD Information Network Operations (DINO) discipline area is responsible for designing, building, configuring, securing, operating, and maintaining and sustaining DoD networks to create and preserve information assurance. DINO is primarily concerned with building and sustaining the network for the purposes of information assurance. Information assurance is defined in DoD Directive (DoDD) 8500.01E as “measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.”[26] DINO enables information assurance, which consequently gives DoD the ability to create, process, and transmit information in a secure fashion denying our adversaries ability to use that information against the United States.

The Defensive Cyber Operations (DCO) discipline area is responsible for conducting passive and active cyberspace operations intended to preserve the ability to utilize the friendly cyberspace capabilities and protect data, networks, and net-centric capabilities. DCO protects DoD networks with an array of tactics, technologies, and procedures which include: multiple layers of defense (defense in depth), multiple factors for security credentialing (common access card with personal identification number), and operating on physically separated networks. Cyber forces employ a host of technologies to assist in the defense of the network such as cryptographically protected interconnected networks (internodal links), passive intrusion detection systems that reports the intrusions, and active intrusion detection systems that take predefined mitigation actions against suspected intrusions. Cyber forces also implement procedures for network defense. These procedures include: end-user security awareness training, civilian training and certification for information technology workers with elevated network privileges, and implementation and use of industry best practices for management of information technology systems.

The Offensive Cyber Operations (OCO) discipline area incorporates all operations conducted to project power against adversaries in or through cyberspace. OCO is force projection with the express intent for conducting offensive operations in the digital/electronic environment. Cyber forces – like their land, sea, air, and space counterparts – are comprised of humans and material solutions: M1A3 Abrams tanks and the tank commander; F22 Raptor and the pilot; submarines and its crew. Cyber forces project combat power against adversaries in or through cyberspace to achieve cyberspace superiority or domination at a time and place of the commander’s choosing.

Cyber forces utilize various tactics and technologies in the application of cyber combat power and force projection. Cyber forces utilize tactics such as zero day attacks, attacking systems that do not have the current patches and hot-fixes applied appropriately, and exploiting known security vulnerabilities to force project combat power against an adversary. After gaining access to the adversary's electronic systems, cyber forces use various technologies to exploit the information environment to achieve the intended effect. The JFC must coordinate, integrate, and synchronize the cyber force operations to achieve the desired effects. The JFC can use the joint functions / warfighting functions to integrate and synchronize cyber forces in the conduct of joint operations.[27]

Warfighting Functions

JP 3-0 defines joint functions as a set of "related capabilities and activities grouped together to help JFCs integrate, synchronize, and direct joint operations."[28] The Army defines the warfighting functions as "a group of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions."[29] The Army's warfighting functions closely align with the joint functions. The Army warfighting functions provide the commander a natural division between the battlefield systems. Each function has its own set of unique tasks, which individually require planning, integration, and synchronization within the function as well as across the other functions. The six warfighting functions with the addition of information and leadership are the elements of combat power. The warfighting functions assist the commander in planning, synchronizing, and executing their missions. The six warfighting functions are: Mission Command, Movement and Maneuver, Intelligence, Fires, Protection, and Sustainment.

JFCs use the warfighting functions to conduct cyber missions tantamount to the more traditional land, sea, air, and space counterparts. The alleged Russian cyber attack on Georgia appropriately illustrates how effective use of Mission Command can result in successful cyber operations. The Army Doctrine Publication (ADP) 3-0 defines Mission Command as a function that “develops and integrates those activities enabling a commander to balance the art of command and the science of control.”[30] The ADP 3-0 further states “commanders drive the operations process through their activities of understand, visualize, describe, direct, lead, and assess…The commander leads the (four primary) staff’s tasks under the science of control.”[31] Cyber electromagnetic activities are one of those four primary staff tasks. The ADP 3-0 defines cyber electromagnetic actions as “activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies both in cyberspace and electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system.”[32] The alleged Russian cyber attack waged against Georgia was controlled and synchronized across the cyber and land domains exemplifying the function of mission command. The Russians spent a significant amount of time planning the execution, identifying target sets to achieve the desired affects, prepositioning assets for execution, and synchronizing the execution to ensure cyber operations transpired in a coordinated fashion in conjunction with the land forces to achieve their national objectives. The offensive cyber operation primarily consisted of a distributed denial of service attack (DDoS), a method of attack that bombards target servers with more traffic than they can effectively handle.[33] In addition to the DDoS attack, observers who watched this play out in cyber space also noted the use of more sophisticated SQL injection attacks, which made the attacks harder to identify because this particular method of attack requires less computers to wage an effective attack.[34] Bringing all this together, the Russians synchronized the cyber attacks by quickly establishing conditions favorable for the ground force invasion. Many of the attacks were so close in time to the corresponding military operations that there had to be close cooperation between the Russian military and the civilian cyber attackers.[35] The intelligence function, especially in the operations process, directly supports the mission command warfighting function.

ADP 3-0 defines the intelligence warfighting function as "the related tasks and systems that facilitate understanding of the enemy, terrain, and civil considerations."[36] The Army Doctrine Reference Publication (ADRP) 3-0 outlines four tasks for intelligence tasks in support of the intelligence warfighting function: "support force generation; support situational understanding; provide intelligence support to targeting and information capabilities; and collect information."[37] Russian cyber forces masterfully worked the intelligence warfighting function to their advantage. The Russian's knew they had the superior force, measured in both numerical force numbers and technologically advanced equipment. Knowing this, Russian intelligence nominated cyber targets not to inflict major catastrophic damage but to cause as much governance and coordination chaos to the Georgian state leadership as possible. The Russians chose targets that included the Georgian presidential website, media, telecommunications, and transportation companies.[38] Although the Russian's could have attacked more strategic targets or key infrastructure via kinetic means, they chose cyber targets that created vast amounts of chaos rather than being totally destructive.

The effects were strategically more of an inconvenience than catastrophic. [39] The Russians chose their targets wisely as seen in retrospect. The Georgian leadership made the decision to move a number of their compromised websites to other countries. For example, Georgia moved their Ministry of Foreign Affairs website to a web-server in the United States in an attempt to escape the DDoS attack and disseminate real-time information by moving to a Blogspot account.[40] This is a case in point of cyber forces moving key assets to a more defensible position, moving and maneuvering in cyberspace from a disadvantaged position to a position of greater advantage.

The movement and maneuver warfighting function is intrinsically about force projection and gaining positional advantage over the enemy. Movement is the repositioning of forces while maneuvering is the combination of force movement and direct fire and close combat. [41] The movement and maneuver warfighting function "is the related tasks and systems that move and employ forces to achieve a position of relative advantage over the enemy and other threats." [42] Cyber forces utilize elements of the movement and maneuver warfighting function to position forces for offensive and defensive operations and reacting to meeting engagements. Russian cyber forces began deploying cyber assets, botnets, as early as two weeks prior to the initial Russian air attacks.[43] In another example of cyber deployment, purported Russian backed cyber forces managed to clandestinely deploy a command and control server in the United States several weeks prior to the initiation of hostilities that helped direct the attack on Georgia.[44] Russian cyber forces employing electronic fires with the DDoS attacks and use of the SQL injection attacks severely affected Georgia's ability to conduct command and control over their internet infrastructure.[45] Georgian cyber forces in response to the unrelenting electronic fires moved the Georgian President's website to a safe location in the United States.[46] The attacks on the Georgian infrastructure would not have been as successful as they were had it not have been for the Russian's leveraging the fires warfighting function.

The ADP 3-0 defines the fires warfighting function as "the related task and systems that provide collective and coordinated use of Army indirect fires, air and missile defense, and joint fires through the targeting process."[47] ADRP 3-0 states, "Army fires systems deliver fires in support of offensive and defensive tasks to create specific lethal and nonlethal effects on a target."[48] Russian cyber forces used the targeting process within the fires warfighting function to identify targets that would disrupt the government and civilian population and appropriately applied the nonlethal fires to create the desired effects. Russian cyber forces used the DDoS attacks as nonlethal fires to harass and create a certain level of chaos within the government and civilian population. Since the intent was never to permanently damage the Georgian electronic infrastructure, the Russian choice to utilize DDoS attacks was most apropos. The targeting selection process could certainly have chosen targets with a more destructive intent, but keeping with the intent to produce inconvenience, harassment, and chaos the targets selected produced the intended effects.

The protection warfighting function deals primarily with force preservation. ADP 3-0 defines the protection warfighting function as "the related tasks and systems that preserve the force so the command can apply maximum combat power to accomplish the mission."[49] ADRP 3-0 further says that protection "determines the degree to which potential threats can disrupt operations and then counters or mitigates those threats."[50]

The Georgian electronic command and control scenario is a perfect illustration of force protection. The perpetrators attacking the Georgian governmental sites were definitely disrupting the Georgian government's ability to provide effective governance. One protection task defined in ADRP 3-0 is applying antiterrorism measures.[51] Russian cyber attackers were able to severely degrade several Georgian webpages including the central government site, the Ministry of Foreign Affairs, the Ministry of Defense, and a number of commercial websites.[52] Georgian Governmental leaders made the decision, once they realized their diminished ability to provide effective governance, to move a number of their web presences to other countries. The Georgian Government, applying antiterrorism measures as a task of the protection warfighting function, moved their Georgian Presidential web presence to the United States.[53]

ADP 3-0 defines the sustainment function as "the related tasks and systems that provide support and services to ensure freedom of action, extend operational reach, and prolong endurance."[54] The alleged Russian cyber attack on Georgia was relatively short in duration, which does not give much need for sustainment operations. However, the best example of sustainment operations in this cyber operation scenario is when the Russian forces produced a limited set of targets and this list eventually made it in to the public space, at the same time, a focused social movement to act on this list began. Russian citizens and Russian sympathizers were motivated to use publicly accessible Denial of Service (DoS) applications to attack the targets on the target list. "The concept is nothing new; in fact, this is state of the art cyber warfare combining all the success factors for total outsourcing of the bandwidth capacity and legal responsibility to the average Internet user. Moreover, next to the "do-it-yourself tools" released, end users who are not so technologically sophisticated are given instructions on how to ping flood Georgian government web sites", thus moving the civilian population with guidance, tools, and resources to accomplish a predefined specific military objective.[55]

As illustrated above, JFCs can (and should) utilize each one of the warfighting functions in the conduct of cyber operations. Cyber forces use them in the same manner as a traditional bridge combat team – in the integration, synchronization, and command and control of cyber operations in the cyber domain. However, the joint functions / warfighting functions are a collection of related activities grouped together to assist the JFC in directing joint operations, the functions are not a substitute for cyber operations doctrine. Cyber leaders certainly need to educate the current force, writ large, utilizing established familiar doctrinal concepts (i.e. joint functions / Army warfighting functions) when and where the doctrine is complementary to the explanation. Yet, the current force is not familiar with the way cyber forces conduct operations – which only adds to the frustration and confusion. To overcome this frustration, the cyber community needs to publish cyber doctrine addressing issues like cyber forces seizing key cyber terrain or cyber forces establishing cyber domain superiority – synonymous to air and maritime supremacy measured in degrees of superiority where opposing forces find themselves incapable of effective interference within the operational area.[56]

Strategic Implications

Doctrine is the "fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application."[57] Doctrine ensures all forces involved in an operation understand where they fit into the plan as well as having a doctrinal understanding of how other forces contribute to the accomplishment of the overall mission. Cyber operations are not so alien that current doctrine proves inadequate in facilitating the integration, synchronization, and mission command of offensive cyberspace operations. The joint functions / Army warfighting functions provide a sufficient framework for integrating and synchronizing offensive and defensive cyber operations across the range of military operations. However, a doctrinal gap does exist around how commanders leverage cyber operations in mission accomplishment.

Doctrine exists for other disciplines concerning their support/contribution to joint operations. The Electro-Magnetic Spectrum Ops Joint Publication 6-01 describes the doctrine for “joint electromagnetic spectrum operations organization, planning, preparation, execution, and assessment in support of joint operations.”[58] The Electronic Warfare Joint Publication 3-13.1 describes the doctrine for “the planning, execution, and assessment of electronic warfare across the range of military operations.”[59] The Military Information Support Operations Joint Publication 3.13.2 “provides guidance for the planning, execution, and assessment of military information support operations in support of joint, multinational, and interagency activities across the range of military operations.”[60] Commanders and staffs may infer from these publications how each operational branch doctrinally executes their mission in support of the larger integrated and synchronized plan. Joint Publication 3-12, Cyberspace Operations, is in development to remedy this capability gap.[61] The Cyberspace Operations publication marks a huge step forward in filling the cyber doctrine gap. The publication published under the 3 series re-enforces that cyber operations are not staff responsibilities but capabilities for commanders to leverage.

The final point with strategic implication is the declaration of what constitutes cyber forces. As the Cyber Operations doctrinal manual codifies how cyber operations are conducted, the question left to answer is what exactly cyber forces look like. Doctrine and force structure delineate what constitutes a Marine Expeditionary Unit or an Army Brigade Combat Team, but we have not yet defined the composition of cyber forces. As illustrated above, cyber operations exist in each of the six joint functions. Cyber forces can and should appropriately leverage capabilities and capacity from the existing supporting functions such as intelligence from the larger intelligence community and the targeting process from the fires community. However, cyber operations are tremendously complex and justifiably require a dedicated force structure to execute their missions. Just what exactly constitutes a cyber force is of great debate right now both within USCYBERCOM and across the service components. Due to the complexities of force structure changes, a Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) study may be required as this would facilitate changes to force structure, potential new material solutions, doctrinal creation and modifications, and training center adjustments just to name a few.[62] JFCs know what comprises an Air Expeditionary Wing or a Carrier Strike Group and to a certain extent, what their capabilities are, but doctrine has not defined to that level of specificity what capabilities cyber forces bring to the fight. Consequentially, joint force planners have great difficulty including cyber operations in their planning for lack of knowledge on cyber force capabilities. As joint doctrine writers continue to develop JP 3-12, Cyberspace Operations, the matter of what constitutes cyber forces must be clearly illustrated – articulating force structure around doctrinal cyber capabilities.

Conclusion

The United States Government over the past two decades has become increasingly dependent on cyberspace to fulfill its governance responsibilities. In 2005, the Department of Defense recognized cyberspace as the fifth operational domain. In 2009, the Commander of U.S. Strategic Command directed the creation of U.S. Cyber Command on the heels of recently reported cyber attacks against Estonia and Georgia. The attacks on Estonia and Georgia highlight the vulnerabilities nations inherently have with greater reliance on cyberspace. These cyber attacks negatively affected the respective state's ability to provide effective governance. Sovereign nations across the world took notice.

This strategic research paper illustrated how JFCs utilize the joint functions / warfighting functions to plan, integrate, synchronize, and command and control offensive cyber operations to achieve intended effects. The cyber mission areas (DINO, DCO, and OCO) are very unique and consequentially do not lend themselves to being inherently cooperative. JFCs use the joint functions / warfighting functions to synchronize cyber operations amongst the three mission areas as well as with the traditional land, air, sea, and space domains, bringing synergy to the joint fight. JFCs use the doctrinal warfighting functions without modification to integrate and synchronize cyber operations to increase synergy in the joint fight. Nonetheless, doctrinal gaps exist preventing commanders at all level from full realization on how to leverage offensive cyber operations. Joint Publication 3-12, Cyber Operations, (currently under development) will close that doctrinal knowledge gap considerably.

Endnotes

[1] Barack Obama, "Remarks By The President On Securing Our Nation's Cyber Infrastructure," May 29, 2009, linked from *The White House Home Page* at "Briefing Room / Speeches and Remarks," http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (accessed January 12, 2013).

[2] U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations,* Joint Publication ver 2.0 (Washington, DC: U.S. Joint Chiefs of Staff, August, 2005), 7.

[3] U.S. Executive Branch, *International Strategy for Cyberspace* (Washington, DC: U.S. Executive Branch, May 2011), 7.

[4] "A Cyber-Riot: Estonia Has Faced Down Russian Rioters. But Its Websites Are Still Under Attack," *The Economist,* May 10, 2007, http://www.economist.com/node/9163598 (accessed November 8, 2012).

[5] Stephen W. Korns, Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Vol 38 (Winter 2008-09), 60.

[6] U.S. Cyber Command Public Affairs, "U.S. Cyber Command," December 2011, linked from *The United States Strategic Command Home Page* at "Organization / Fact Sheets," http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed November 10, 2012).

[7] Ibid.

[8] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,"* Joint Publication 1-02 (Washington DC: U.S Joint Chiefs of Staff, November 15, 2012), 77.

[9] U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations,* 7.

[10] Ibid., 16.

[11] Ibid., 7.

[12] Ibid., 8.

[13] Bonnie N. Adkins, *The Spectrum of cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?,* Air Command and Staff College, Air University Research Report (Maxwell Air Force Base, AL: U.S.A.F. Air Command and Staff College, April 2001), 26.

[14] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* 268.

[15] GEN Keith B. Alexander, "CYBERCOM Posture Statement," Congressional Record (March 20, 2012).

[16] Dorothy E. Denning, "Activitism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," n.d.,

http://www.prgs.edu/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf (accessed November 4, 2012).

[17] John Quaid, "European Climate Exchange Site Hacked," July 27, 2010, linked from *The Financial Services Technology Home Page* at "Latest News" http://www.fsteurope.com/news/European-Climate-Exchange-site-hacked/ (accessed November 11, 2012).

[18] Dorothy Denning, "Statement of Dorothy E. Denning," May 23, 2000, linked from *The Federation of American Scientists Intelligence Resource Program Home Page* at "Intelligence Resource Program / Congressional Material" http://www.fas.org/irp/congress/2000_hr/00-05-23denning.htm (accessed November 11, 2012).

[19] Ibid.

[20] Kim Zetter, "H(ackers)$_2$O: Attack on City Water Station Destroys Pump," November, 18, 2011, linked from *Wired Home Page* at "Wired Security / Threat Level" http://www.wired.com/threatlevel/2011/11/hackers-destroy-water-pump/ (accessed November 11, 2012).

[21] Ibid.

[22] U.S. Department of the Army, *Unified Land Operations*, Army Doctrine Reference Publication 3-0 (Washington, DC: U.S. Department of the Army, May 16, 2012), 3-1.

[23] U.S. Joint Chiefs of Staff, *Joint Operations,* Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), GL-7.

[24] U.S. Army Cyber Command, *United States Army Cyber Command, Army Land Cyber White Paper, 2012-2030,* (Fort Meade, MD: U.S. Army Cyber Command, September 14, 2012), 6.

[25] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* 177.

[26] U.S. Department of Defense, *Information Assurance,* Department of Defense Directive 8500.01E (Washington DC: U.S. Department of Defense, April 23, 2007), 17.

[27] U.S. Joint Chiefs of Staff, *Joint Operations,* III-1.

[28] Ibid.

[29] U.S. Department of the Army, *Unified Land Operations*, Army Doctrine Publication 3-0 (Washington, DC: U.S. Department of the Army, October 10, 2011), 13.

[30] Ibid., 13.

[31]Ibid., 13.

[32] U.S. Department of the Army, *Unified Land Operations*, ADRP 3-0, 3-3.

[33] John Markoff, “Before the Gunfire, Cyberattacks,” August 12, 2008, linked from *The New York Times Home Page* at “Technology,” http://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed November 18, 2012).

[34] Dancho Danchev, “Coordinated Russia vs Georgia Cyber Attack in Progress,” August 11, 2008, linked from *The ZDNet Home Page* at “Security,” http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 (accessed November 18, 2012).

[35] John Bumgarner, Scott Borg, “Overview by The US-CCU of The Cyber Campaign Against Georgia in August of 2008,” August, 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf (accessed November 18, 2012).

[36] U.S. Department of the Army, *Unified Land Operations*, ADP 3-0, 14.

[37] U.S. Department of the Army, *Unified Land Operations*, ADRP 3-0, 3-4.

[38] Markoff, “Before the Gunfire, Cyberattacks,”.

[39] Steve LeVine, “Cyber-Attack Strategy: Part of Russian Attack on Georgian Pipelines: Report Finds,” August 24, 2009, linked from *The Energy Bulletin Home Page* at “Stories,” http://www.energybulletin.net/stories/2009-08-24/cyber-attack-strategy-part-russian-attack-georgian-pipelines-report-finds (accessed November 18, 2012).

[40] Danchev, “Coordinated Russia vs Georgia Cyber Attack in Progress,”.

[41] U.S. Department of the Army, *Unified Land Operations*, ADRP 3-0, 3-3.

[42] U.S. Department of the Army, *Unified Land Operations*, ADP 3-0, 14.

[43] Markoff, “Before the Gunfire, Cyberattacks,”.

[44] Ibid.

[45] Ibid.

[46] Danchev, “Coordinated Russia vs Georgia Cyber Attack in Progress,”.

[47] U.S. Department of the Army, *Unified Land Operations*, ADP 3-0, 14.

[48] U.S. Department of the Army, *Unified Land Operations*, ADRP 3-0, 3-4.

[49] U.S. Department of the Army, *Unified Land Operations*, ADP 3-0, 14.

[50] U.S. Department of the Army, *Unified Land Operations*, ADRP 3-0, 3-5, 3-6.

[51] Ibid.

[52] Danchev, “Coordinated Russia vs Georgia Cyber Attack in Progress,”.

[53] Ibid.

[54] U.S. Department of the Army, *Unified Land Operations*, ADP 3-0, 14.

[55] Danchev, “Coordinated Russia vs Georgia Cyber Attack in Progress,”.

[56] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* 13, 192.

[57] Ibid., 95.

[58] U.S. Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations,* Joint Publication 6-01 (Washington DC: U.S. Joint Chiefs of Staff, March 20, 2012), i.

[59] U.S. Joint Chiefs of Staff, *Electronic Warfare,* Joint Publication 3-13.1 (Washington DC: U.S. Joint Chiefs of Staff, February 8, 2012), i.

[60] U.S. Joint Chiefs of Staff, *Military Information Support Operations,* Joint Publication 3-13.2 (Washington DC: U.S. Joint Chiefs of Staff, February 8, 2012), i.

[61] “Joint Doctrine Hierarchy,” November 20, 2012, linked from *The Defense Technical Information Center Home Page* at “Status,” http://www.dtic.mil/doctrine/doctrine/status.pdf (accessed December 28, 2012).

[62] Chairman of the Joint Chiefs of Staff, *Joint Capabilities Integration And Development System,* Chairman of the Joint Chiefs of Staff Instruction 3170.01H (Washington DC: Chairman of the Joint Chiefs of Staff, January 10, 2012), 2.